PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-260902
(43)Date of publication of application : 29.09.1998

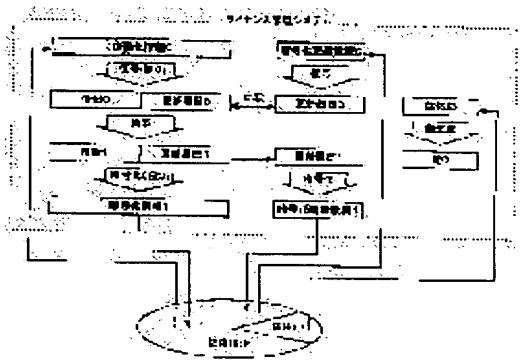
(51)Int.Cl. G06F 12/14
G06F 12/14

(21)Application number : 09-065073
(22)Date of filing : 18.03.1997

(71)Applicant : FUJITSU LTD
(72)Inventor : YOSHIMOTO SHINICHI

(54) INFORMATION PROTECTING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To make it difficult to forge information.
SOLUTION: A recording medium which is given a specific recognition symbol characteristic is provided with a 1st area where information and its update history are recorded and a 2nd area where the update history is recorded and only when the update history recorded in the 1st area matches with the update history recorded in the 2nd area, the information is allowed to be updated. For this constitution, the 2nd area may be provided on another recording medium. Or a cipher key obtained from the specific recognition symbol characteristic of the recording medium is used to cipher and record the information on the recording medium and the cipher key is changed for every time the information is updated.



LEGAL STATUS

[Date of request for examination]	13.03.2001
[Date of sending the examiner's decision of rejection]	16.08.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－260902

(43)公開日　平成10年(1998)９月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ
	３２０		３２０Ｂ

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願平9－65073

(22)出願日　平成９年(1997)３月18日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　吉本　真一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　井桁　貞一

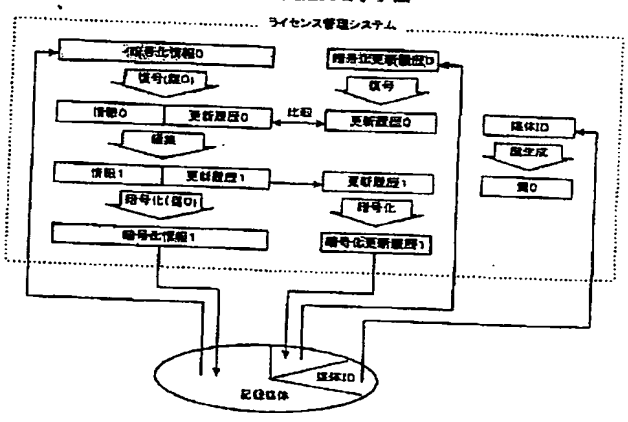
(54)【発明の名称】　情報保護方法

(57)【要約】

【課題】　情報保護方法に関し、情報の改ざんの困難化を目的とする。

【解決手段】　記録媒体固有の認識記号が付された記録媒体に、情報と該情報の更新履歴とを記録する第１の領域と、前記更新履歴を記録する第２の領域とを設け、前記第１の領域に記録されている更新履歴と、前記第２の領域に記録されている更新履歴とが一致する場合に限って、前記情報の更新を許容するように構成する。また、前記構成において、第２の領域を別の記録媒体に設けるように構成することも可能である。或いは、記録媒体固有の認識記号から得られた暗号鍵を用いて、情報を暗号化して該記録媒体に記録し、前記情報を更新する毎に該暗号鍵を変更するように構成する。

第１の実施例を示す図



1

【特許請求の範囲】

【請求項１】　記録媒体固有の認識記号が付された記録媒体に、情報と該情報の更新履歴とを記録する第１の領域と、前記更新履歴を記録する第２の領域とを設け、前記第１の領域に記録されている更新履歴と、前記第２の領域に記録されている更新履歴とが一致する場合に限って、前記情報の更新を許容することを特徴とする情報保護方法。

【請求項２】　記録媒体固有の認識記号が付された第１の記録媒体に、情報と該情報の更新履歴とを記録する領域を設け、第２の記録媒体に前記更新履歴を記録する領域を設け、前記第１の記録媒体に記録されている更新履歴と、前記第２の記録媒体に記録されている更新履歴とが一致する場合に限って、前記情報の更新を許容することを特徴とする情報保護方法。

【請求項３】　記録媒体固有の認識記号から得られた暗号鍵を用いて、情報を暗号化して該記録媒体に記録し、前記情報を更新する毎に該暗号鍵を変更することを特徴とする情報保護方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報保護方法に係り、特に不正ユーザによる改ざん行為から，著作物等の重要情報を保護する方法に関するものである。

【０００２】

【従来の技術】現在、ソフトウェアやコンテンツは、インターネットや可換媒体（フロッピーディスクやCD-ROM）を通じて流通しており、可換媒体に記録されたソフトウェアやコンテンツを、コンピュータシステムに接続されているHDD にインストールする場合、個々のインストーラは、ソフトウェアやコンテンツの著作権を保護するため、ソフトウェアやコンテンツのインストールを制限する機能を備えている。具体的には、インストール先コンピュータシステムを限定したり、またはインストール回数を制限したりする機能である。

【０００３】一方、ソフトウェアやコンテンツの著作権を保護するもう一つの動きが、媒体IDを用いて、媒体上のソフトウェアやコンテンツを保護する方法である。次に媒体IDを使用したコンテンツの保護方法の具体的な一例を示す。

(1) コンテンツの暗号化

適当な暗号鍵Ｋでコンテンツを暗号化し、記録媒体に保存する。

(2) 許諾コード

暗号鍵Ｋを許諾コードへ変換する。ここでは、記録媒体の媒体IDを暗号鍵として用いて、暗号鍵Ｋを暗号化し、許諾コードを得るものとする。許諾コードは、コンテンツの所有者が、コンテンツ使用を許可したコンテンツ使用者にのみ与えるものとする。

(3) コンテンツの使用

2

コンテンツを使用するためには、まず、コンテンツの所有者からコンテンツ使用許可をもらい、許諾コードを得ることが必要である。許諾コードが得られた場合、記録媒体の媒体IDを暗号鍵として用いて、許諾コードを復号し、暗号鍵Ｋを得る。さらに、得られた暗号鍵Ｋを用いて、暗号化されたコンテンツを復号することで、始めてコンテンツが使用可能となる。

【０００４】上記に示したコンテンツの保護方法は、記録媒体毎に異なる媒体IDを用いているという特徴がある。このため、コンテンツを使用するには、コンテンツが保存されている記録媒体毎に許諾コードを必要とする。

【０００５】例えば、記録媒体Ａ用許諾コードを持ったコンテンツ使用者が、コンテンツを記録媒体Ａから記録媒体Ｂに複写し、記録媒体Ｂに保存されたコンテンツを使用しようとして、記録媒体Ａ用許諾コードを用いたとしても、コンテンツは使用できないのである。記録媒体Ｂに保存されたコンテンツを使用するには、記録媒体Ｂ用の許諾コードを必要とする。記録媒体Ａ用許諾コードしか持たないコンテンツ使用者は、記録媒体Ａ上でしかコンテンツの使用を許可されないのである。

【０００６】著作権保護方法によっては、個々のコンテンツに応じた許諾コードを要求するものがある。このような方法では、コンテンツ利用毎に許諾コードをいちいち入力するのは面倒なので、コンテンツ初回利用時には許諾コードを要求し、入力された許諾コードを所定の形式で記録しておき、次回コンテンツ利用時には記録しておいた許諾コードを利用して、許諾コード入力の手間を省く機能を備えている場合が多い。

【０００７】インストーラによる保護方法、および媒体IDを用いた保護方法において、不正ユーザによる改ざん行為から保護しなければならない情報がある。インストーラの場合は、インストール先コンピュータシステムを識別する情報（例えば、マシンIDやネットワークアドレス等）や、インストール回数等がそれである。媒体IDを用いた著作権保護方法では、許諾コードに関する情報がそれである。現在これらの情報は、記録媒体上の通常は使用しない領域に記録したり、通常使用する領域に記録したとしても暗号化して記録するなどしている。

【０００８】

【発明が解決しようとする課題】以上説明した従来の情報保護方法においては、情報の記録場所が既知であり、情報変更ツールがあれば、情報の改ざんは容易に実現できるという問題点があった。例えば、情報の改ざんによって、インストール先コンピュータシステムを変更したり、インストール回数を変更したりすることが可能であった。

【０００９】本発明は以上のような情報の改ざんを容易に行えない情報保護方法の提供を目的としたものである。

3

【００１０】
【課題を解決するための手段】第１の手段は、記録媒体固有の認識記号が付された記録媒体に、情報と該情報の更新履歴とを記録する第１の領域と、前記更新履歴を記録する第２の領域とを設け、前記第１の領域に記録されている更新履歴と、前記第２の領域に記録されている更新履歴とが一致する場合に限って、前記情報の更新を許容することである。すなわち、情報が改ざんされたか否かを検査して、改ざんされていない場合に限って、前記情報の更新を認める。なお、記録媒体と記録媒体固有の認識番号とは、必ずしも一対一に対応するとは限らず複数媒体に同一の認識番号を付す場合も含む。
【００１１】第２の手段は、記録媒体固有の認識記号が付された第１の記録媒体に、情報と該情報の更新履歴とを記録する領域を設け、第２の記録媒体に前記更新履歴を記録する領域を設け、前記第１の記録媒体に記録されている更新履歴と、前記第２の記録媒体に記録されている更新履歴とが一致する場合に限って、前記情報の更新を許容することである。
【００１２】第３の手段は、記録媒体固有の認識記号から得られた暗号鍵を用いて、情報を暗号化して該記録媒体に記録し、前記情報を更新する毎に該暗号鍵を変更することである。
【００１３】
【発明の実施の形態】本発明を適用した第一の実施例について述べる。図１に、ソフトウェアやコンテンツのライセンスを管理するライセンス管理システムの機能の一部と、著作権を保護するための情報（インストーラによる著作権保護方法においては、インストール先コンピュータシステムを識別する情報またはインストール回数をさし、媒体IDによる著作権保護方法においては、許諾コード等の情報をさす。以下、重要情報と略す）を記録する記録媒体を示す。ライセンス管理システムは、データの暗号化および復号化機能、暗号鍵（以下、鍵と略す）を生成する機能、記録媒体より媒体IDを読み出す機能、重要情報の読出しおよび書込み機能、重要情報が更新される毎に更新される更新履歴の読出しおよび書込み機能から構成される。さらに、インストーラによる著作権保護方法においては、インストールの実行許可を与えるか否かを判定する機能、媒体IDによる著作権保護方法においては、ソフトウェアやコンテンツの利用許可を与えるか否かを判定する機能を備えている。
【００１４】ライセンス管理システムにおいて、重要情報の更新要求が発生した場合、重要情報の更新は以下の手順で行われる。
(1)記録媒体から媒体IDを読出し、媒体IDから所定のアルゴリズムにより鍵０を生成する（図４に示す固定鍵を用いた暗号アルゴリズムやハッシングアルゴリズムの出力データ、または単に媒体IDと固定値との排他的論理和の結果を、鍵０としてもよい）。

4

【００１５】(2)記録媒体から暗号化された重要情報（図１では暗号化情報０）を読み出す。
(3)鍵０を用いて暗号化情報０を所定の暗号アルゴリズムにより復号し、重要情報（図１では情報０）と更新履歴０との組を得る。
【００１６】(4)暗号化された更新履歴（図１では暗号化更新履歴０）を記録媒体から読み出す。なお、記録媒体上における更新履歴の記録領域は、重要情報が記録されている領域とは別の領域とする。たとえば、記録媒体上に構築されたファイルシステムが使用しない領域、ヒドゥンセクタあるいはリザーブ領域などがよい。
【００１７】(5)所定の暗号アルゴリズムを用いて暗号化更新履歴０を復号し、更新履歴０を得る。また更新履歴を暗号化せずに平文のまま記録しておいた場合には、復号する必要はない。
【００１８】(6)（3)で得た情報０と更新履歴０との組に含まれる更新履歴０と、(5)で得た更新履歴０とを比較し、同一の場合は処理を続行する。それ以外の場合は重要情報に対し不正な改ざんが行われたことになるので、処理を中断する。
【００１９】(7)重要情報を情報０から情報１に更新し、それに伴い、更新履歴１を作成して情報１に添付する。なお、更新履歴については、重要情報を更新する毎に、更新した回数、更新日時、更新後の重要情報のサイズなどの項目を記録し、過去から現在まで重要情報の更新履歴とする。また、過去から現在までの更新履歴を記録してもよいが、現時点の項目だけを記録してもよい。またハッシングアルゴリズム（図４）を用いて、現時点の項目に対応したデータを生成して、このデータを記録してもよい。
【００２０】(8)鍵０を用いて、情報１と更新履歴１との組を所定の暗号アルゴリズムにより暗号化して、暗号化情報１を得る。暗号化する際には、情報１と更新履歴１を一つの塊として考え、暗号アルゴリズムとしては、DES におけるCBC 、CFB またはOFB モード等を用いて、暗号化するのがよい。
【００２１】(9)暗号化情報１を記録媒体に記録する。
(10)（7）で得た更新履歴１を、情報１と更新履歴１との組とは別に所定の暗号アルゴリズムにより暗号化して、暗号化更新履歴１を得る。また暗号化せずに平文のまま記録媒体に記録する場合は、暗号化の必要はない。
【００２２】(11）暗号化更新履歴１を、記録媒体上に構築されたファイルシステムが使用しない領域、ヒドゥンセクタあるいはリザーブ領域などに記録する。
次に、本発明を適応した第二の実施例について述べる。
【００２３】図２に、ライセンス管理システムの機能の一部と、ライセンス管理システムとは伝送路（インターネットなど）を介して接続されているライセンス管理センタと、重要情報を記録する記録媒体１を示す。
【００２４】ライセンス管理センタは、媒体IDによる著

5

作権保護方法において、ソフトウェアやコンテンツの著作権所有者が、ユーザに対してソフトウェアやコンテンツを利用する許可を与えるとき、ソフトウェアやコンテンツを利用するときに必要とされる許諾コードを発行する役割を果たす。

【００２５】ライセンス管理システムが、ライセンス管理センタより許諾コードを受け取ったのち、記録媒体１に記録されている重要情報（許諾コード管理表）を更新する必要がある。その手順は以下のとおりである。

【００２６】(1)ライセンス管理システムは、ライセンス管理センタに、ユーザが所望するソフトウェアやコンテンツを利用するための許諾コードを要求する。

(2)ライセンス管理センタは、ユーザに対してソフトウェアやコンテンツを利用する許可を与えるか否かを、ソフトウェアやコンテンツの著作権所有者に問い合わせる。

【００２７】(3)ライセンス管理センタは、許諾コードを生成する。

(4)ライセンス管理センタは、以前許諾コードを発行したときにライセンス管理システムから受信した暗号化更新履歴０を、記録媒体０から読み出す。

【００２８】(5)ライセンス管理センタは、許諾コードと暗号化更新履歴０をライセンス管理システムに送信する。これより、以下のようにライセンス管理システム側の処理となる。

【００２９】(6)記録媒体１から媒体IDを読出し、媒体IDから所定のアルゴリズムにより鍵０を生成する（図４に示す固定鍵を用いた暗号アルゴリズムやハッシングアルゴリズムの出力データ、または単に媒体IDと固定値との排他的論理和の結果を、鍵０としてもよい）。

【００３０】(7)記録媒体１から暗号化された重要情報（図２では暗号化情報０で示す）を読み出す。

(8)鍵０を用いて暗号化情報０を復号し、重要情報（図２では情報０、具体的には許諾コード管理表）と更新履歴０との組を得る。

【００３１】(9)ライセンス管理センタから受信した暗号化更新履歴０を、所定の暗号アルゴリズムを用いて復号し、更新履歴０を得る。また更新履歴を暗号化せずに平文のままライセンス管理センタに送信しておいた場合には、復号する必要はない。

【００３２】(10)（8）で得た情報０と更新履歴０との組に含まれる更新履歴０と、(9)で得た更新履歴０とを比較し、同一の場合は処理を続行する。それ以外の場合は重要情報に対し不正な改ざんが行われたことになるので、処理を中断する。

【００３３】(11)重要情報を情報０から情報１に更新し、それに伴い、更新履歴１を作成して情報１に添付する。なお、更新履歴は、重要情報を更新する毎に、更新した回数、更新日時、更新後の重要情報のサイズなどの項目を記録し、過去から現在まで重要情報の更新履歴と

6

する。また、過去から現在までの更新履歴を記録してもよいが、現時点の項目だけを記録してもよい。またハッシングアルゴリズム（図４に示す）を用いて、現時点の項目に対応したデータを生成して、このデータを記録してもよい。

【００３４】(12)鍵０を用いて、情報１と更新履歴１との組を所定の暗号アルゴリムにより暗号化して、暗号化情報１を得る。暗号化する際には、情報１と更新履歴１を一つの塊として考え、暗号アルゴリズムとしては、DESにおけるCBC、CFBまたはOFBモード等を用いて、暗号化するのがよい。

【００３５】(13)暗号化情報１を記録媒体１に記録する。

(14)(7)で得た更新履歴１を、情報１と更新履歴１との組とは別に所定の暗号アルゴリズムにより暗号化して、暗号化更新履歴１を得る。また暗号化せずに平文のままライセンス管理センタに送信する場合は、暗号化の必要はない。

【００３６】(15)暗号化更新履歴１を、ライセンス管理センタに送信する。ここまでがライセンス管理システム側の処理である。

(16)ライセンス管理センタは、ライセンス管理システムより受信した暗号化更新履歴１を記録媒体０に記録する。

【００３７】続いて、本発明を適応した第三の実施例について述べる。図３に、ライセンス管理システムの機能の一部と、重要情報を記録する記録媒体を示す。

【００３８】ライセンス管理システムは、記録媒体より媒体IDを読み出す機能、データの暗号および復号機能、媒体IDより暗号鍵を決定する際に用いられるパラメータの読出しおよび書込み機能、暗号鍵を生成する機能、暗号鍵を検査する際に用いる情報を生成する機能、重要情報の読出しおよび書込み機能などから構成される。さらに、インストーラによる著作権保護方法においては、インストールの実行許可を与えるか否かを判定する機能、媒体IDによる著作権保護方法においては、ソフトウェアやコンテンツの利用許可を与えるか否かを判定する機能を備えている。

【００３９】ライセンス管理システムにおいて、重要情報の更新要求が発生した場合、重要情報の更新は以下の手順で行われる。

(1)記録媒体から媒体IDとパラメータ０を読出し、パラメータ０を用いた所定のアルゴリズムにより、媒体IDから鍵０を生成する（パラメータ０を暗号鍵として用いた暗号アルゴリズムを適用したり、または単に媒体IDとパラメータ０との排他的論理和を鍵０としてもよい）。なお、記録媒体上におけるパラメータの記録領域は、重要情報が記録されている領域とは別の領域とする。たとえば、記録媒体上に構築されたファイルシステムが使用しない領域、ヒドゥンセクタあるいはリザーブ領域などが

よい。

【００４０】(2)記録媒体から暗号化された重要情報（図３では暗号化情報０）を読み出す。

(3)鍵０を用いて暗号化情報０を所定の暗号アルゴリムにより復号し、重要情報（図３では情報０）と暗号鍵を検査するための情報（図３では鍵検査情報０）との組を得る。

【００４１】(4)所定のアルゴリズムにより鍵検査情報０を生成する。なお、鍵検査情報については、ライセンス管理システム内に変化しない重要情報IDを内部変数として保存しておき、重要情報IDを鍵検査情報として用いる方法、また、固定値を暗号鍵として用いた暗号アルゴリズムやハッシングアルゴリズム（図４）を用いて、重要情報に対応した圧縮したデータを鍵検査情報として用いる方法などがある。

【００４２】(5) (3)で得た情報０と鍵検査情報０との組に含まれる鍵検査情報０と、(4) で得た鍵検査情報０とを比較し、同一の場合は処理を続行する。それ以外の場合は重要情報に対し不正な改ざんが行われたことになるので、処理を中断する。

【００４３】(6)重要情報を情報０から情報１に更新する。

(7) (4)で用いたアルゴリズムにより鍵検査情報１を生成して、情報１に付加する。

【００４４】(8)乱数発生アルゴリズムによりパラメータ１を生成し、そのパラメータ１を用いて、(1) で用いたアルゴリズムにより媒体IDから鍵１を生成する。

(9)鍵１を用いて、鍵検査情報１との組を所定の暗号アルゴリムにより暗号化して、暗号化情報１を得る。

【００４５】(10) 暗号化情報１を記録媒体に記録する。

(11) パラメータ１を、記録媒体上に構築されたファイルシステムが使用しない領域、ヒドゥンセクタあるいはリザーブ領域などに記録する。

【００４６】最後に、本発明を適応した第四の実施例について述べる。基本的には第三の実施例と同様の構成であるが、第二の実施例にあるように、媒体IDより鍵を生成する際に用いるパラメータをライセンス管理システム側の記録媒体に記録するのではなく、ライセンス管理センタ側の記録媒体に記録する構成としてもよい。

【００４７】

【発明の効果】以上の説明から明らかなように、本発明によれば従来の情報保護法方では防止することができなかった情報の改ざん、例えば、情報の改ざんによって、インストール先コンピュータシステムを変更したり、インストール回数を零回に変更したりすることを回避することができる。

【図面の簡単な説明】

【図１】　第１の実施例を示す図。

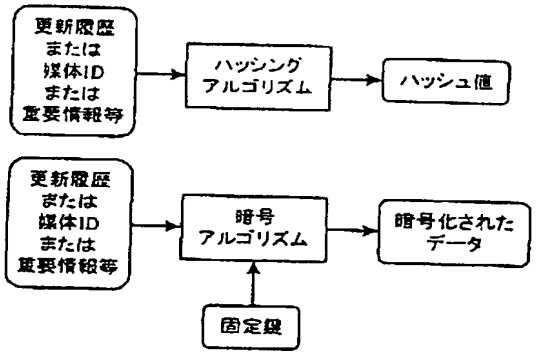
【図２】　第２の実施例を示す図。

【図３】　第３の実施例を示す図。

【図４】　使用アルゴリズムの例を示す図。

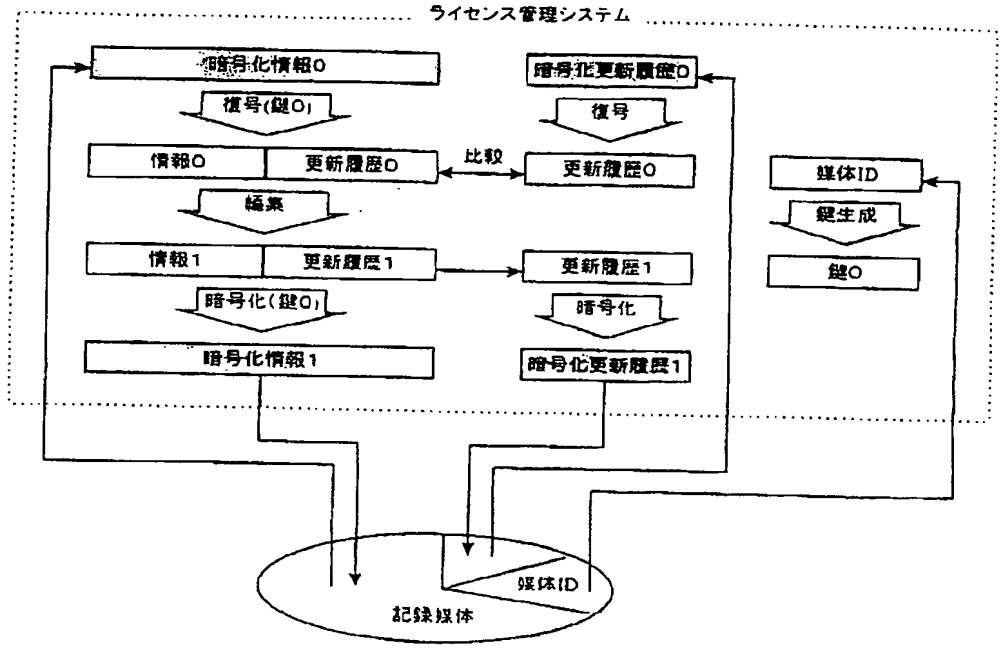
【図４】

使用アルゴリズムの例を示す図



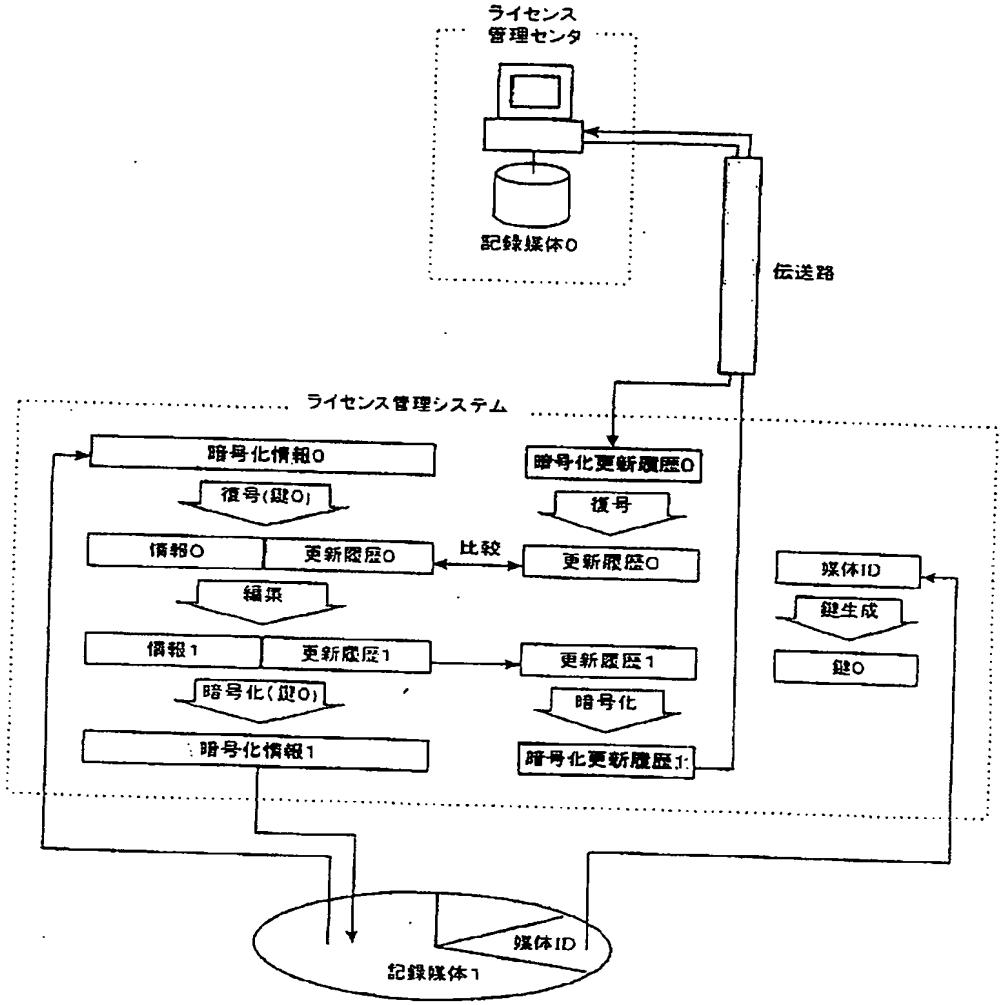
【図１】

第１の実施例を示す図



【図２】

第２の実施例を示す図



【図３】

第３の実施例を示す図